European Commission

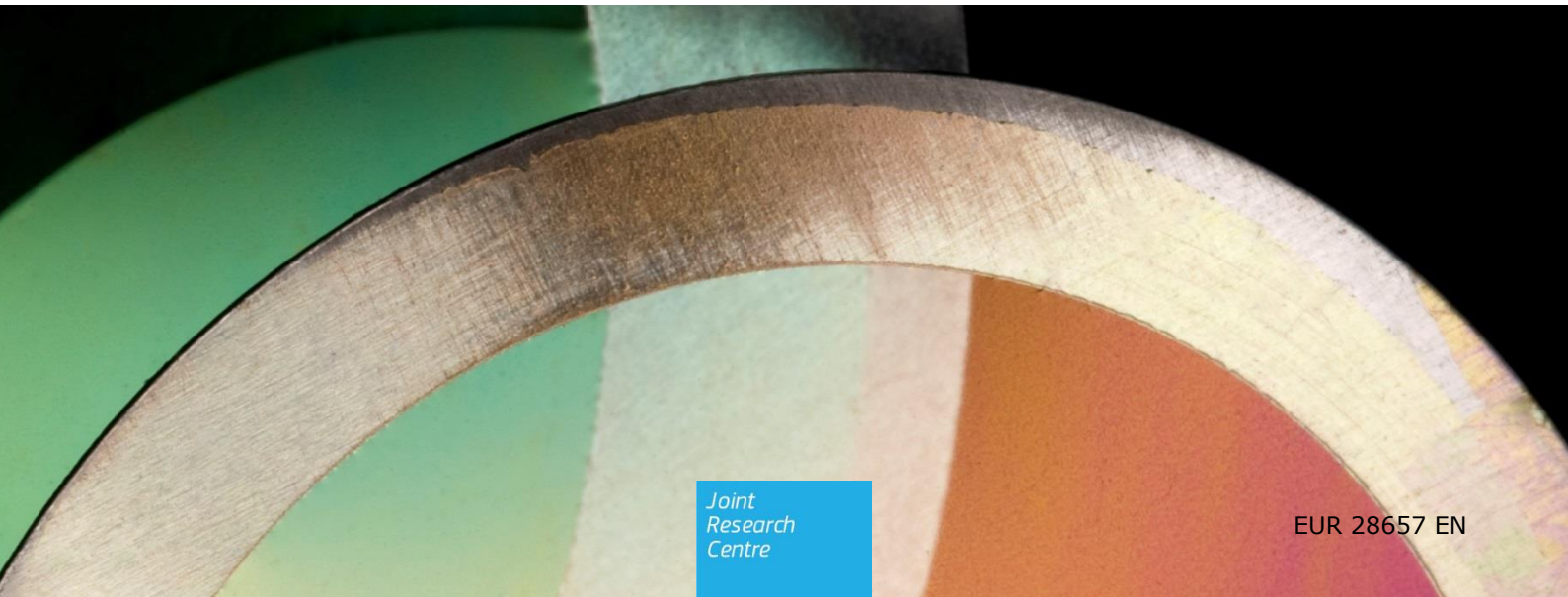
JRC TECHNICAL REPORTS

ERNCIP training for professionals in critical infrastructure protection: from risk management to resilience

The ERNCIP's roadmap and lessons learned from design to execution

A. LAZARI

2017



Joint Research Centre

EUR 28657 EN

Contact information
Name: Alessandro Lazari
Address: Via E. Fermi 2749, 21027 — Ispra (Va) — Italy
Email: alessandro.lazari@ec.europa.eu
Tel. +39 0332 786244

JRC Science Hub
https://ec.europa.eu/jrc

JRC105204

EUR 28657 EN

PDF	ISBN 978-92-79-69731-9	ISSN 1831-9424	doi:10.2760/932771
Print	ISBN 978-92-79-69730-2	ISSN 1018-5593	doi:10.2760/88009

Luxembourg: Publications Office of the European Union, 2017

How to cite this report: Lazari, A., *ERNCIP training for professionals in critical infrastructure protection: from risk management to resilience,* EUR 28657 EN, Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-69731-9, doi:10.2760/932771, JRC105204.

Contents

Abstract

This report, about the ERNCIP pilot course on 'Training for professionals in critical infrastructure protection: from risk management to resilience', contains an analysis of the roadmap followed by the Joint Research Centre (JRC) in establishing, in cooperation with DG Migration and Home Affairs, a first-of-its-kind training event strongly based on the European programme for critical infrastructure protection (EPCIP). This deliverable contains references to all the steps involved in this project; its conceptualisation, the validation of its functional requirements and modules and its final execution in Brussels from 21 to 23 June 2016.

The aim of this document is to disseminate the methodologies and material collected during the execution of the project and provide useful references, topics and suggestions to educators and trainers — and their organisations — that are willing to organise or fine-tune courses on critical infrastructure protection and resilience with a focus on European policies and strategies.

The ERNCIP's goal, following the publication of this report, is to receive feedback from institutions and experts that have made use of the course materials with a view to integrating them in such courses in the future.

The course materials could also be used by DG Migration and Home Affairs as one of the actions put in place to foster the improvement of the 'external domain' of the EPCIP. The fact that the EPCIP also aims at reaching out to neighbouring countries of the European Union, with a view to establishing CIP-related forms of cooperation, puts the course among the most useful and direct tools to be exploited to achieve such an objective.

Figure 1. Some participants in the ERNCIP pilot course for professionals

in critical infrastructure protection

Acknowledgements

The author would like to acknowledge the efforts and assistance of the following colleagues and experts. Without their multidisciplinary and multifaceted contributions, the ERNCIP pilot course would not have seen the light of day. The author would like to thank Prof. Enrico ZIO, Dr John AGIUS and Dr Alois SIEBER for their great support in the organisation and execution of the course.

European Commission staff:

Eva-Maria Engdahl (DG Migration and Home Affairs)

Torben Fell (DG Migration and Home Affairs)

Karl-Johan Forsberg (JRC)

Peter Gattinesi (JRC)

Georgios Giannopoulos (JRC)

Maria Giovanna Giuliani (JRC)

Daniele Kashani-Rad (JRC)

Naouma Kourti (JRC)

Georg Peter (JRC)

Christer Henrik Pursianen (JRC)

Gian Luigi Ruzzante (JRC)

Marianthi Theocharidou (JRC)

ERNCIP Academic Committee:

Jacqueline Akvahan (Cranfield University — United Kingdom)

William Guy Billotte (National Institute of Standards and Technology — United States)

Herve Borrion (University College of London — United Kingdom)

Katya Delak (National Institute of Standards and Technology — United States)

Pierre-Alan Fonteyne (Université Catholique de Louvain — Belgium)

Janusz Górski (Politechnika Gdanska — Poland)

Christie Jones (George Mason University — United States)

Jennifer Marshall (National Institute of Standards and Technology — United States)

Alois Sieber (Chairman of the ERNCIP Academic Committee)

Bengt Sundelius (Uppsala University — Sweden)

Paul Theron (Thales Group — France)

Mark Troutman (George Mason University — United States)

Enrico Zio (Politecnico di Milano — Italy)

Focus Group with Operators:

Martin Bilek (C.E.P.S. — Czech Republic)

Andrea Chittaro (Snam — Italy)

Francisco Javier Garcia Carmona (Iberdrola — Spain)

Gerald McQuaid (Vodafone — United Kingdom)
José Pires (U.I.C. — France)
Jean-Luc Planchet (SNCF Reseau — France)
Sarah Taylor (Centrica — United Kingdom)

Lecturers:
Martin Bilek (C.E.P.S. — Czech Republic)
Andrea Chittaro (Snam — Italy)
Piotr Ciepiela (Ernst & Young)
Georgios Giannopoulos (JRC)
Georgios Koutepas (Unisystem)
Christie Jones (George Mason University — United States)
Nicolae Merla (Centre for Coordination of Critical Infrastructure Protection — Romania)
Kurt Misak (Austrian Power Grid — Austria)
Jean-Luc Planchet (SNCF Reseau — France)
Marianthi Theocharidou (JRC)
Paul Theron (Thales Group — France)
Enrico Zio (Politecnico di Milano — Italy)

Panel of Observers:
John Agius (Critical Infrastructure Protection Directorate — Malta)
William Billotte (National Institute of Standards and Technology — United States)
Georgios Eftychidis (KEMEA Centre for Security Studies — Greece)
Christie Jones (George Mason University — United States)
Robert Mikac (DUZS — Croatia)
Eduard Mračka (Ministry of Transport and Construction — Slovakia)
Roberto Setola (Unicampus — Italy)
Alois Sieber (Chairman of the ERNCIP Academic Committee)
Vasileios Theofilopoulos (Hellenic Police Astynomia — Greece)

1 The ERNCIP training course for professionals in critical infrastructures protection

Held in Brussels from 21 to 23 July 2016, the pilot ERNCIP training course for professionals in critical infrastructure protection was organised with two main purposes in mind: sharing the technical experience around the EPCIP and the ECI directive (114/08/EC) — on consolidated concepts like the operator security plan (OSP), the security liaison officer (SLO) and the 'transboundary externalities' — and exploiting the course as a potential tool for the continued enhancement of the existing European CIP community.

The organisation of the training has put in place some pivotal factors that have made this experience the first of its kind: the focus on the EPCIP, the joint DG Migration and Home Affairs/JRC involvement and the horizontal exploitation of the ERNCIP's network of contacts in the domain of CIP, built over more than 7 years of the project's lifecycle. Through the ERNCIP's network, in fact, many experts, participants, observers and lecturers have been reached, confirming the adaptability of the European Reference Network for Critical Infrastructure Protection also beyond its core activities.

The course's 3-day timetable has been designed to provide an incremental experience through CIP-specific topics — from risk management to resilience — and to prepare the ground for a table-top exercise to be held on the last day. The decision to schedule the exercise on the last day has proven to be a successful move, as the first 2 days of lectures and discussions enabled all the participants to get acquainted with each other and for mutual trust between them to be fostered — all elements that then facilitated the execution of the exercise.

The experience, in its embryonic concept, was aimed at mid-career security managers operating in the sectors of energy and transport, as the course was strongly inspired by the EPCIP and aimed at consolidating experiences around its implementation and execution. In the end, the 20 participants — mostly with between 5 and 8 years of experience and with a profile of risk analyst or business continuity officer — came exclusively from the energy sector and were equally distributed between the sub-sectors of electricity and gas.

The final organisation of the course took this last element into consideration, by inviting lecturers and experts that could share experiences and analyse scenarios mainly related to the energy sector. The transport sector, however, was not completely excluded from the agenda as one full lecture including a use case was given during the course with excellent feedback as it helped to draw comparisons between the operational and security-related needs of infrastructures operating in different domains that have strong dependency from the energy sector.

With a view to maximising the output of the pilot course, the ERNCIP Office, in agreement with DG Migration and Home Affairs, decided to establish a Panel of Observers. The idea was to involve a group of experts and give them the duties of 'auditing' the execution of the course, providing comments and feedback for a potential new iteration of the course, and finally to be ready to provide further insights and elements during the lectures and discussions following them. The role of the Panel of Observers has gone way beyond the aforementioned list of expectations, as the experts have actively participated in the course and have also had a major role in facilitating the execution of the exercise.

Such a result could only be achieved by involving a mixed matrix of representatives of Member States, academics and subject matter experts that provided a 360 ° multidisciplinary coverage in terms of experience, opinions and case studies. Due to enduring cooperation agreements covering scientific and technical topics, two non-EU experts were involved in the Panel of Observers and this element also added an international dimension to the overall experience, thanks to the possibility of hearing about the experiences of a country with a different CIP state of play. Such circumstance

also enabled the participants to compare different approaches to similar issues, accidents and events related to critical infrastructures.

The aim of this document is to disseminate ERNCIP's roadmap and lessons learned, from design to execution of the course, together with the material (slides, exercise scenario and multimedia) provided by the lecturers, so as to provide useful references and suggestions to educators and trainers — and their organisations — that are willing to organise or fine-tune courses on critical infrastructure protection and resilience with a focus on European policies and strategies. All the presentations and the scenario for the exercise will be made available in a dedicated section of the ERNCIP website so that anyone with an interest in CIP can have access to them.

The ERNCIP Office's goal, following the publication of this report, is to receive feedback from institutions and experts that have made use of the course materials with a view to integrating them in the execution of new iterations of training events.

1.1 The agenda of the course

The course was executed according to the following agenda.

DAY 1 — 21 June 2016

Opening of the course

- N. Kourti — European Commission — Joint Research Centre — Directorate E. 'Space, Security and Migration'
- T. Fell — European Commission — DG Migration and Home Affairs, Unit D.1

Introduction to the course on CIPR ([1])

- G. Giannopoulos — European Commission — Joint Research Centre — Directorate E. 'Space, Security and Migration'

MODULE 1 — Complex systems analysis, modelling and simulation ([2])

- Prof. E. Zio — Politecnico di Milano

MODULE 2 — Risk Assessment

- 'Risk assessment methodologies for critical infrastructure protection'
  - M. Theocharidou — European Commission — Joint Research Centre — Directorate E. 'Space, Security and Migration'
- 'Risk management for critical infrastructures'
  - P. Cipiela — Ernst and Young Business Advisor

TEAM WORK on use cases with use of the GRRASP tool ([3])

- G. Giannopoulos and M. Theocharidou — European Commission — Joint Research Centre — Directorate E. 'Space, Security and Migration'

([1]) Prior to the course, the attendants were invited to check the CIPEDIA platform, to review the glossary of most common terms used in the field of CIP.

([2]) This module was aimed at reviewing the availability of tools and models and how they can support the operators' mission in enhancing prevention, preparedness and response to disruptive events. The lecture also provided an overview of complexity and how it can be modelled and simulated, also through practical examples and scenarios.

([3]) This module was carried out as a table-top exercise on how to implement a holistic approach to prevention, preparedness and response vs business continuity. The case studies were developed by operators. The GRRASP tool is available here: https://ec.europa.eu/jrc/en/grrasp/download

DAY 2 — 22 June 2016

Introduction to the second day and what to expect

- G. Giannopoulos — European Commission — Joint Research Centre — Directorate E. 'Space, Security and Migration'
- Prof. E. Zio —Politecnico di Milano (Italy)

MODULE 3 — The cyber dimension

- 'Towards a general theory of resilience: lessons from a multi-perspective research' — P. Theron — Thales Group;
- 'Cyber risk management in industrial control systems' — G. Koutepas — Unisystem S.A.

MODULE 4 — Risk assessment, management and incident response

- Gas distribution: 'Security risk management. from prevention to response' plus a case study on a 'terrorist attack on a dispatching centre ([4])' — A. Chittaro — Head of Corporate Security — SNAM (Italy)
- Electricity transmission: 'High-impact low-frequency events on energy grids plus a case study on cascading effects on the energy grid based on real incidents' — K. Misak — Austrian Power Grid (Austria)
- Urban transport: 'Operational risk management plus a case study on an explosion of a transformer close to an underground's control centre' — J. L. Planchet — SNCF Reseau (France)

MODULE 5 — The security liaison officer

- 'The security liaison officer and lessons learned from exercises' — M. Bilek — CEPS (Czech Republic)

MODULE 6 — The international dimension

- 'Critical infrastructure protection and resilience in the US' — C. Jones — Center for Critical Infrastructure Protection and Homeland Security — George Mason University (Virginia — United States)

DAY 3 — 23 June 2016

Introduction to the third day and presentation of the Panel of Observers

- J. Agius — Critical Infrastructure Protection Directorate (Malta)
- A. Lazari — European Commission — Joint Research Centre — Directorate E. 'Space, Security and Migration'

([4]) The Dispatching Centre operates and continually monitors the gas transmission system so that gas quantities are available at any time and at any point of the network. This work is carried out by the operations room at the Dispatching Centre which is staffed 24 hours a day by specialised personnel. The remote-control stations located in this room are staffed by operators who make forecasts, enact simulations and carry out remote control checks. The room has a large synoptic display panel showing the national gas pipeline network.

MODULE 5a — The operator security plan

'Governmental perspective on the OSP and an assessment of the state of play after the promulgation of OSP-related laws and regulations'

- N. Merla — Centre for Coordination of Critical Infrastructure Protection (Romania)

Roundtable: Operators' perspectives on the operator security plan

- Participants: M. Bilek (CEPS), A. Chittaro (SNAM), N. Merla (Centre for Coordination of Critical Infrastructure Protection — Romania), K. Misak (Austrian Power Grid — APG), J. L. Planchet (SCNF), R. Setola (UniCampus)

Team work on cross-sectorial table top exercises ([5])

- Facilitators: E. Zio (Politecnico di Milano), G. Giannopoulos, A. Lazari, M. Theocharidou (European Commission — Joint Research Centre — Directorate E. 'Space, Security and Migration)

Open discussion on the solutions to the cross-sectorial exercises and lessons learned

- Moderator: A. Sieber
- Facilitators: Panel of Observers, M. Bilek (CEPS), A. Chittaro (SNAM), K. Misak (Austrian Power Grid — APG), J. L. Planchet (SCNF)

After each session and module of the course, the participants were given some time to discuss specific items arising from the presentation and get answers not only from the lecturers, but also from the members of the Panel of Observers, who were also engaged in the discussion and provided their perspective and shared their direct experiences.

This resulted in very intense and detailed discussions around key topics that had already been identified as the core of the course. Among them, particular care was dedicated to the concepts of risk, resilience, transboundary externalities, operator security plans (OSPs) and security liaison officers (SLOs).

1.2 The table-top exercise.

The table-top exercise, apart from testing the experience and team work of the participants, was meant to stimulate/assess the following elements:

- increasing the awareness of sector and cross-border issues;
- putting the participants in a condition to tackle a certain scenario without 'rejecting' it;
- identifying participants' reactions if the accident is escalated to other Member States;
- fostering the need for the participants to ask themselves: *'Do you need to coordinate? How? Who would you get in touch with?'.*

The following scenario was used for the exercise.

Energy companies hit by the BlackEnergy malware

([5]) This session was dedicated to the solution of one cross-sectorial exercise prepared with the support of the Panel of Observers. The 20 attendants were split into two groups and given one exercise per group. The aim of the exercises was to test the interoperability of the expertise and experience of experts coming from different fields of the European domain. The experts were requested to agree on a possible solution (or set of solutions) to deal with a certain scenario. Another aim of the exercise was to assess the extent to which the response to certain events was converging toward a harmonised approach.

On 23 2016, a major malware attack affects power transmission companies in Europe and results in the disruption of services in many regions across EU, with cascading effects also in neighbouring countries of the EU. The malware controls and then disables workstations involved in the control of transmission and distribution systems. There are also indications that this was a rather coordinated attack.

Technical details

The malware uses a number of Windows-related vulnerabilities to spread. In its latest appearance, the victims receive Microsoft Office files that are supposed to contain useful information but require the activation of macros. Once initiated, the macros install a component which communicates with the attackers and downloads additional modules as required.

The additional module destroys system files with the purpose of incapacitating infected systems. It also corrupts a vast array of file types, making them irretrievable. In this particular case, researchers also find that it is particularly searching for processes and files associated with industrial control functions.

In the latest identified incidents, it seems that the main purpose of the attackers is disruption of operations. Nevertheless, researchers have also found that in some cases the malware establishes an access point in the infected systems installing a Secure Shell (SSH) server. The remote access opens the possibility that attackers may try to infiltrate and control the power system rather than just disrupting it.

Affected systems — Extent of the problem

This malware manages to disrupt the energy transmission and distribution (gas and electricity) in various regions across EU. More than 100 million inhabitants (across five countries and in different areas) do not have access to electricity and gas. The pattern of the disruptions is random within the affected countries and across the EU. This renders it even more difficult to identify the systems that have initially been affected, which is another additional burden for forensics.

In addition, other companies may have been affected although no disruptions have occurred in their networks. What is unique in this situation is that both ICS and ICT systems are affected. The modularity of the attack vector raises additional concerns for future attacks.

Issues to be discussed

#Within the organisation

Effective protection of critical infrastructures demands a holistic and strategic approach as the basis for a comprehensive protection strategy and requires a truly interdisciplinary agenda encompassing fields from engineering to computer science and policy research/decision-making. All the aspects need to be addressed and this all-inclusive approach employing a combination of solutions should be considered when facing a wide range of possible vulnerabilities. It is obvious that all of these aspects are at the different stages of development and levels of implementations — some are enforced, while others are just a set of suggestions; they come in various shapes and forms across diverse communities which sometimes do not agree on the exact nature of the problem or on what assets need to be protected with which measures.

- Who would be involved from the upper management in the response phase? How important is the involvement of the upper management?
- Both ICS and ICT systems are affected. Do you have a unique cybersecurity entity in the organisation or should these issues be addressed by different departments? If so, how would you assure a smooth collaboration during this emergency considering that ICT and ICS staff have different objectives and mentalities?
- How can you overcome disagreements and unify procedures internally?

Technical issues

The priorities of any ICT department are usually confidentiality, integrity and availability. On the contrary the priorities for the ICS are availability, integrity and confidentiality. Different staff members within an organisation support each system with different mentalities. This results in a difference in fundamental approaches leading to conflicting technical and operational differences between ICS and ICT that need to be addressed.

- What technical measures have been implemented in your company to reduce the impact and prevent cyberattacks Do you see this situation reflected in cross-sector operations and cooperation?
- Do you already have a plan in place to face a situation of this magnitude? If not, how would you react?
- Disruptions of your services have affected a neighbouring EU Member State. How do you deal with this issue in order to re-establish the service? Have you got a pre-established mechanism for quick intervention?

Information sharing

- How can you bring this up between interconnected and/or interdependent operators in the same country and across the EU?
- What procedures are in place in order to share information with the authorities at national and international level?
- How do you communicate the event and the loss of service to the public? Do you use social media?

Strategic planning in the aftermath of the event

- Is there an internal audit process that will be followed in the aftermath of the event in order to identify weaknesses that led to these adverse events?
- Are internal training courses in place in order to disseminate lessons learned?
- Do you foresee a public dissemination of the event investigation in order to contribute to the information-sharing process and better planning for the whole sector across the EU?
- Do you feel that your corporate risk insurance has updated frameworks to cover these kinds of disruptions? How effective and efficient could be the approach of risk transfer through insurance?

1.3 Questions and topics that triggered a discussion during the course

After each lecture or round table, the participants and the panel were given time to discuss specific questions arising from the topic being covered.

What follows is a list of questions that were raised and discussed during the course. The availability of this list seems to be an important element to be taken into consideration, and if similar courses are to be organised, coverage of them could be included in the lectures (or in pre-course reading material) or at least they could be expected and a detailed response provided.

A list of 'key findings' is also provided to enable the further fine-tuning of experiences from this project and to provide a deeper insight on what was discussed during the course.

#Questions raised after the lecture: 'Complex systems analysis, modelling and simulation':

- Is there a way to validate these models?
- How to find a balance between performance and resilience?
- Is there any link between preparedness and resilience in the simulation models?
- How to make simulation tools available also to smaller operators?
- How to share information properly between provider and client?

#Questions raised after the lecture: 'Risk assessment methodologies for critical infrastructure protection':

- Are there any good practices in the field of crisis management, related to CIPR, to be shared?

#Questions raised after the lecture: 'Risk management for critical infrastructures':

- Is CERT's advice working in both the ICT and ICS fields?

#Questions raised after the lecture: 'Security risk management: from prevention to response, plus a case study on a terrorist attack to a dispatching centre':

- How do you organise training internally?
- Do you conduct exercises with other organisations?
- What is the balance between security and costs?
- Do you have any modelling and simulation structure in place?

#Questions raised after the lecture: 'The security liaison officer and lessons learned from exercises':

- How many times do you revise the OSP and the procedures related to the OSP?
- What language is used during cross-border exercises?

#Questions raised after the lecture: 'Operational risk management plus a case study on an explosion of a transformer close to an underground's control centre':

- Do you have a document describing your operational governance?
- How do you define the motivation of the attackers?

- Do you receive any information from the authorities?
- Do you think that too much security may affect the performance of the system?

#On the execution of exercises and on the usage of modelling tools:

- Exercises should should enable stakeholders to gain new awareness on how to run their introspection analysis.
- During exercises, all communication and notification protocols and devices should be carefully tested.
- Modelling tools should be run on past incidents as a way to review real cases and validate the simulations' assumptions.

#On the operator security plans and on costs of security:

- Security is felt to be a cost but in fact is a tool for companies to gain competitive advantage. The ability to operate in risky conditions to be able to cope with them means gaining advantage.
- It took long internal discussions to convince the board of directors to invest in training and provide awareness-related material over the company's intranet.
- The company develops very specific security plans in cooperation with the governments and around those assets that are vital for keeping a certain sector operative.
- The grid-restoration section is the biggest part of the OSP with a focus on supra-regional, regional and local grids.
- The list of people to be contacted in case of crisis is sensitive information within the OSP.

#On the operational lifecycle:

- 'You need to verify that employees absorb the automations in order to react.'
- Agreements are crucial to put on paper the objectives of cooperation between operators and first responders or law enforcement. Communication with law enforcement also needs to be fostered through giving the operators access to dedicated communication devices and networks that are normally used by law enforcement.
- The 'security by design' comes after the infrastructure has been deployed and has started operating. Injecting new security measures is more difficult in old/obsolete infrastructures.

1.4 Key findings during the execution of the exercise

The execution of the exercise was an important part of the course as it called for the extensive use of the participants' previous expertise and experiences.

These were not the only elements exploited by the participants, as they referred also to the lecture slides to deal with the issue described by the scenario. This circumstance implies that they had absorbed fresh new knowledge during the training course and that they felt comfortable enough to apply it straight away.

Some of the aspects covered by the groups' discussions will be summarised in the following. The intention is to provide further insight into elements that characterised the execution of the exercise and that made it a successful experience, also if considering that the participants haven't 'rejected' the scenario. It is common, in fact, that table-top exercises containing too imaginative scenarios may lead to the participants rejecting them, as they may be perceived as 'unrealistic'.

In the case reviewed by this report, the scenario was well received by the participants and led to interesting discussions and to sharing of multi-faceted experiences.

One of the challenges faced by the participants was the one that requested them to apply some filters to clarify their role in the scenario. They had to take some time to discuss how to tackle the scenario and from which angle, also because of the variety of expertise and sub-sectors represented in the exercise-room.

That was not the only challenge faced, as the participants successfully managed to discuss the key topics requested by the exercise and also found time to discuss the following elements:

- restoring the last-available backup to recover IT and/or OT platforms;
- data integrity and forensics;
- communications with the government if the usual channel are compromised;
- commuting to manual operations if automation control systems fail;
- damage assessment and availability of alternative and/or redundant systems;
- what to do if the accident is happening for the first time or there is no contingency plan to cope with that circumstance;
- forensics reports are also necessary for insurance-related evaluation of damages.

1.5 Feedback from participants and observers.

The training course was attended by a total of circa 40 people (20 participants and 20 experts divided between lecturers and members of the Panel of Observers), working in the domain of European CIP. The outcome was perceived as quite positive as the mid-career security managers attending the course confirmed that, indeed, they had gained new knowledge and improved understanding that they could immediately benefit from, in the execution of their critical infrastructure protection and resilience duties.

Feedback collected by all the attendants during the course can be summarised as follows.

- (Some) have never faced a relevant incident/accident in their working life and therefore have no experience and/or are not prepared to face events of a certain magnitude.
- During the execution of the course and the exercise, they felt tested on a multidimensional level of safety, security and protection.
- (Some) admitted that cross-border incidents are outside their experience.
- Participants got a clear explanation of why resilience is so important.
- (Some) faced the exercise by using 50 % experience and 50 % knowledge acquired during the 3-day course.
- Participants came back home with the idea of executing similar exercises in their companies as they had never had experiences like this one.
- The multidimensional and multinational discussion was very useful and mind-opening.
- Team work with other professionals was beneficial.
- The scenario could have had more specificity.

- During the exercise, many points of view converged toward an agreed solution.
- The exercise required participants to invest some time in finding a common tune.
- (Some) thought that the primary goal of the exercise was not to solve the issue but to share views.
- '*It was important to get to know each other and recognise that we are surrounded [by] and dependent [on] other providers/operators.'*

Observers provided the following feedback.

- The topics covered by the course are focused on improving security managers' capabilities.
- The exercise was a good experience as the participants didn't fight against the scenario.
- The scenario should have included some more coordinates in order to make the expected result clearer.
- The exercise was beneficial as many European approaches were discussed and this would have an impact (in terms of awareness) at national level.
- The course was an opportunity to exchange experiences; more time for the exercise should have been allocated and a more detailed timeline of the evolution of events should have been included.
- The course could have had fewer lectures and a little more time for open discussions.

All the participants also provided feedback through an 'event feedback form'. Some of their responses are collected below.

- '*Excellent course … presentations would probably be interesting for a Point of Contact meeting.' ([6])*
- *'Very good and useful course, well structured and (most important) with much knowledge disseminated/exchanged with much applicability for the next day-to-day businesses.'*
- '*Even when the academic part (day 1) was sometimes hard to follow, it is still useful because of the rare occasions to get in contact with this information (e.g. modelling). Also very interesting [was] the speaker from United States to learn from their practices. Could be a kind of periodical training course for SLOs to keep up with recent developments both in the scientific field [and in] legal and operator practices.'*
- '*On day 1 there was too much theory — it would be lovely to see how academic approach is put into action.'*
- *'Day 2 was too long.'*
- '*More time needed on case studies and security risk assessment.'*
- '*Keep up the good work'.'*
- '*The start point of the exercise should be defined beforehand allowing a jump start. A lot of time was lost due to discussions ranging from 'we need to find out what happened' to 'now we are post event, everything is restored, so we are analysing what happened.'*

([6]) 'Point of Contact meeting' refers to the biannual meeting with representatives of Member States, organised by DG Migration and Home Affairs in the context of the EPCIP.

- *'The positive aspect of this exercise is that people became aware of the need for cross-border cooperation, not only on the national level (authorities) but also on the TSO level. Within the companies, Transmission System Operators (TSOs) do have disaster recovery plans available, but it seems like there is some gap for cross-border/multi-TSO preparations. This shows that the interdependencies between different TSOs, different sectors and countries becomes more and more important'.*

1.6 Lessons learned

The goal of this section is to provide some suggestions and elements that could easily be considered as a response to the question: '*What would I amend or add, if I had to organise this course again?'*.

The organisation of the pilot training required many elements to be put into place: the development of the curriculum, the interaction with relevant stakeholders for its validation, the recruitment of the lecturers, attendants and observers and, finally, the execution and logistics of the course.

These processes allowed the ERNCIP Office to improve its knowledge and awareness on many aspects related to the organisation of a training course and, furthermore, to learn the ones that are pivotal for the organisation of a successful and fruitful experience. They can be summarised as follows.

Something that should never be underestimated is **the venue**. The venue must allow easy interaction between all the stakeholders, as the goal of a training course shouldn't be only the one of passing knowledge to the participants, but also the one of letting them interact and share experiences and multiple perspective points of view.

The need for easy interaction has to be well taken care of, and therefore the training room should be fully equipped with multimedia capabilities (video and audio streaming through projector and speakers) and should allow participants and lecturers to adequately see each other. Another important aspect is the one of allowing enough room for the lecturer(s) to move in front of the audience and throughout the entire length of the images displayed by the projector. This is very important as the interaction will be maximised if the lecturer can get close to the audience and become part of the 'video stream', to emphasise certain elements of the presentation or multimedia being reproduced.

Concerning **the content** of the course and the agenda, the first lesson that can be reported is that a new iteration of the same course would include fewer lectures to allow much more time for discussion. Following some lectures, in fact, the participants engaged in interesting and fruitful discussions that had to be interrupted prematurely due to the need to respect the course's schedule.

The discussions between participants and lecturers are a very important part of the overall experience, particularly if they are analysing technical details that are pivotal for the comprehension of certain protocols or best practices. Considering that the participants were engaged with topics like the 'trans-boundary' issues between EU Member States, the operator security plans and the figure of the security liaison officer, the discussions on these matters could have been allocated a lot more time to allow further exchanges and sharing of personal experiences. In the next iteration, specific sessions will be organised to allow maximisation of this specific element of the course.

A very successful element was the number of **participants**. The 20 participants were given enough time to interact with the lecturers and observers (also during lunch and coffee breaks). A higher number would have made the course less manageable, perhaps even chaotic, and could possibly have reduced the trust building among the participants. In the pilot course, the focus was on infrastructures operating in the European domain, on the EPCIP's pillars and on mid-career security managers. The course was carefully built around these three elements in view to delivering a dedicated experience.

The issue of the 'available **time**' called for a semi-flexible management of every day's agenda. All the lectures were delivered according to the schedule but the discussion following them had sometimes to be interrupted, to stay within the time limits.

The time issue leads to some considerations regarding the execution of the **exercise**. The course incorporated one exercise to be performed in the second half of the last day. This solution worked well as by that time participants had managed to get acquainted with each other and had developed an initial trust. However two elements should be considered if events like this one are being organised in the future.

- An entire day (and not a half) might be allocated to the final exercise, to allow careful dissection of the elements requested by the exercise and also to 'measure' how much the participants have 'metabolised' and applied the topics being discussed during the course.
- An opening exercise might be organised to compare how much preparation the participants already had at the beginning of the course and compare it with the results obtained from last day's exercise.

Looking at the reactions and interactions witnessed during the exercise, the goal of the 'metabolisation of knowledge' was surely reached as the participants very often referred to the lectures for providing a solution to certain issues. This goal's achievement is surely due to the lecturers' capability in highlighting priority elements to be considered and to the scenarios being covered (deeply linked to real operational issues and procedures).

Still on the issue of 'time', a last lesson learnt will be reported. This course was 'designed' as a 3-day experience, as this was perceived as the 'maximum' amount of time that companies would have allowed for course. Whether this assumption was true or not, it's the author's opinion that a course like this would be better organised in the form of a summer school or 'CIP lab' and over the time of 5 days. The coverage of delicate elements pertaining to the European dimension of CIP, together with the need to cover many aspects that require focus, suggests a schedule with a more relaxed pace together with the inclusion of social events to foster trust building and, most importantly, to boost the consolidation of a European CIP community.

2 A brief introduction to the ERNCIP

The 'Directorate Space, Security and Migration' (previously named the Institute for the Protection and the Security of the Citizen) of the Joint Research Centre of the European Commission set up the European Reference Network for Critical Infrastructure Protection (ERNCIP) project in 2009. This took place under the mandate of the Directorate-General for Migration and Home Affairs, in the context of the European programme for critical infrastructure protection (EPCIP), and with the agreement of Member States. The preparatory phase was successfully completed in November 2010 and the project started its implementation phase in 2011.

Since then, the ERNCIP Office, established at the Joint Research Centre, has looked after the administration, governance and dissemination of the project's outcomes.

The ERNCIP aims at providing a framework within which experimental facilities and laboratories share knowledge and expertise to harmonise test protocols throughout Europe, leading to better protection of critical infrastructures against all types of threats and hazards.

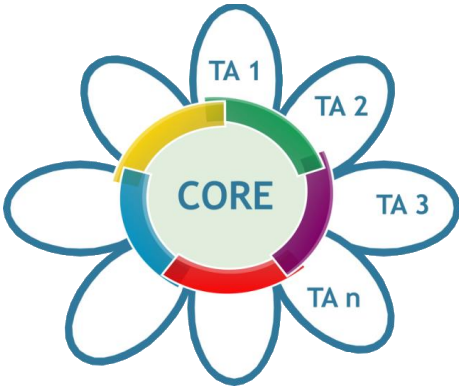


Figure 2. The ERNCIP thematic areas as the core activity of the ERNCIP

The work of the ERNCIP is mainly supported by thematic groups (Figure 1) composed of European subject-matter experts that facilitate the accomplishment of the project's mission: 'to foster the emergence of innovative, qualified, efficient and competitive security solutions, through the networking of European experimental capabilities'.

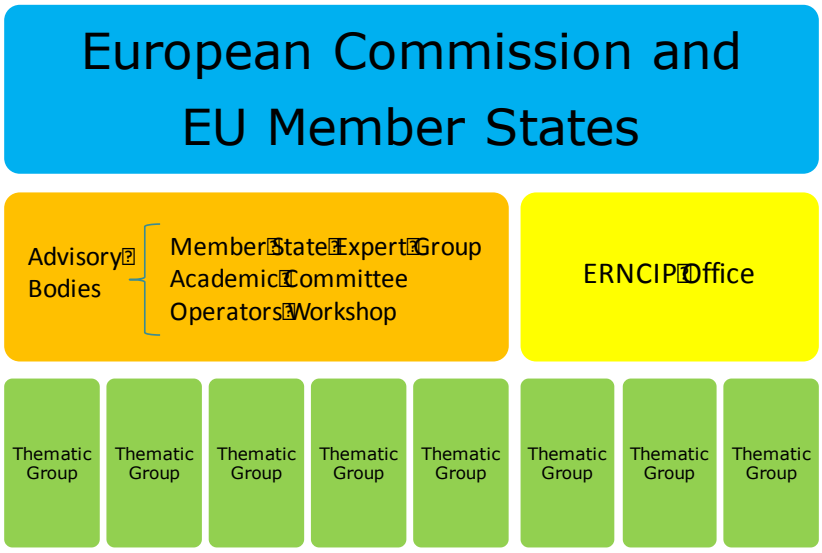


Figure 3. The organisational structure of the ERNCIP project

Additionally, the ERNCIP has established advisory bodies (Figure 2) representing different stakeholder groups. These groups have been established in view to discussing and considering the perspectives of infrastructure operators, academia, EU Member States, directorates-general of the European Commission (e.g. DG Migration and Home Affairs and DG Communications Networks, Content and Technology), EU agencies and other bodies (e.g. the European Union Agency for Network and Information Security — ENISA) and European and international organisations.

They include the following:

— the Operators' Workshop (usually taking place once a year);

— the ERNCIP Group of EU CIP Experts (usually meeting twice per year);

— the Academic Committee.

3 The ERNCIP Academic Committee

The Academic Committee (AC) has had a central role in the design of the modules of the pilot project. It has been established as a multidisciplinary advisory body to the ERNCIP Office and the thematic groups. In that capacity, it has an important role to play as a link between academia and the ERNCIP. It also aims to be a forum for discussion on how to further develop CIP-related knowledge in the academic community.

The Members of the AC have been chosen from among renowned senior scientists or academic specialists in fields relevant to the ERNCIP. Technical and social sciences as well as humanities have been considered and included. The ERNCIP has also ensured that the AC's members have considerable knowledge of major European and other funding programmes, and are also representative in terms of Member States as well as gender balance.

The role of the AC is to discuss and give strategic advice to the ERNCIP Office and thematic groups on the following issues:

- Horizon 2020 and other research and funding programmes relevant to the ERNCIP;
- the latest scientific developments and research results in the fields related to the ERNCIP;
- possible new fields of interest for the ERNCIP to consider;
- general risk assessment and risk management issues related to the ERNCIP;
- ethical issues related to the ERNCIP;
- outcomes of the thematic groups and evaluation of the ERNCIP as a whole;
- relevant documents produced within the ERNCIP project;
- other strategic-level issues related to the ERNCIP.

The AC, as already stated above, has played a major role in the development and execution of the ERNCIP pilot training course as the embryonic concepts regarding this project were initially discussed and consolidated during its meetings held at the JRC's site in Ispra (Italy) in 2014/2015.

4 Embryo stage: the factors that triggered the organisation of the ERNCIP course

The factors that triggered the evaluation of training and education as items to be included in the ERNCIP's agenda were, in particular, the discussions taking place during the AC meeting of 8 April 2014 and the second ERNCIP Operators' Workshop of 19 and 20 May 2014.

4.1 Academic Committee meeting of 8 April 2014

The AC, having the intention to proactively promote a feasibility study on the establishment of a 'qualified training for European professionals in CIPR', intensively discussed the following item: 'From national CIP education towards common curricula?'.

The intention was to invite the participants to discuss whether there would be benefits from creating or harmonising a European curriculum in CIP–related education, and if so, how to get there.

The following main arguments and information were put forward in the discussion.

- There is a mismatch between university education and industry needs. The answer lies in looking at the needed functions and then working out the essential competencies to develop 'standards' for capabilities (focusing on operators, supervisors, managers, etc.).
- Benchmarking a security programme would be good, but the needs and objectives have first to be developed, and it is unclear who should do it.
- The need of universities and training centres to acquire requirements and suggestions for preparing courses on CIPR (from under/postgraduate education to training).

The meeting ended with the following recommendations and actions for the future.

- 'The AC recommends that the potential CIP-related education requirements of CI operators, especially about the ways to identify the essential competences, are sought during the ERNCIP Operators' Workshop in May 2014'.
- A group of AC members should articulate their ideas on CIP-related education into short concise arguments (half a page) by the next AC meeting (20 and 21 October 2014).
- Moderators at the ERNCIP Operators' Workshop should be briefed to include the identification of potential CI operator-related education requirements within the reports on their sessions.

4.2 Second ERNCIP Operators' Workshop of 19 and 20 May 2014

The call for the ERNCIP's action in the field of training and education was further reinforced by the discussions and recommendations provided by operators and subject-matter experts, during the second ERNCIP Operators' Workshop (https://erncip-project.jrc.ec.europa.eu/documents/second-erncip-operators-workshop-workshop-report).

The participants discussed the following topics.

- Even if many offers of certified security training for operators exist — mostly national or even (enterprise or sector-specific) proprietary and independent solutions — the underlying requirements are not harmonised and a cross-border or mutual recognition as certified professionals is not yet established.
- In the area of risk assessment, a scenario-oriented view — applicable for multiple purposes such as training, risk assessment, security testing and validation — is still not applied. Existing and successfully used safety features might be transferred or transformed to security ones, which would require a better understanding of risk assessment, in order to distinguish between safety and security risks.
- In the area of risk awareness, a wide range of information and related tools, and project results, are publicly available. Nevertheless there is still a lack of qualified training in relation to risk awareness in different areas. This concerns education/training in both the academic environment and in business schools. These challenges include the manager's need for better understanding of risks in order to be better prepared for decision-making. The speed of change and the related fast developments result in greater dependencies between people and processes/systems within the knowledge base.
- Regarding the issue of providing guidance and support to CIP operators, simulation and training events are tools that are very much needed. It is indispensable to practise case scenarios (normally threat scenarios) on the basis of the currently available instruments in order to learn how to improve them, to understand better how to use them and to know what is missing — all in a collaborative way among operators.

The discussion of the aforementioned topics led to the formulation of the following recommendation:

'[The] ERNCIP to facilitate the creation of such an EU-wide harmonised training scheme for CI operators' staff. The training scheme should include training on realistic threat scenarios and vulnerabilities of CIs, meaning that an applied, hands-on approach should be favoured.'

5 Links with EU policy and strategies

Following the AC meeting of 8 April 2014 and the second ERNCIP Operators' Workshop on 19 and 20 May 2014, the ERNCIP Office, as for every new item or action to be considered and possibly eventually pursued, promoted an internal discussion and research to look for consistent links with relevant EU policy and strategies, in view to promote the initialisation of a new work stream and find partner DGs interested in supporting it.

The research had a positive result as 'training' — intended as tool for fostering and improving the protection and resilience of critical infrastructures within the European Union — was clearly considered as a potential driver in the following official documents and directives:

- Commission Staff Working Document SWD(2013) 318 final on a new approach to the European programme for critical infrastructure protection ([7]);
- CBRNE Action Plan ([8]) 'Action4 — goal 4: 'improve training' ([9]).

Training was also mentioned in Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, and more specifically in:

- Article 8 'Commission support for ECIs'

  '*The Commission shall support, through the relevant Member State authority, the owners/operators of designated ECIs by providing access to available best practices and methodologies as well as support training and the exchange of information on new technical developments related to critical infrastructure protection.'*;

- Annex II 'ECI OSP procedure'

  …The ECI OSP procedure will cover at least: …

  3. identification, selection and prioritisation of counter-measures and procedures with a distinction between:

  — permanent security measures, which identify indispensable security investments and means which are relevant to be employed at all times. This heading will include information concerning general measures such as technical measures (including installation of detection, access control, protection and prevention means); organisational measures (including procedures for alerts and crisis management); control and verification measures; communi-cation; awareness raising and training; and security of information systems.'

These findings led to a preliminary discussion with DG Migration and Home Affairs — long-term partner, founder of the ERNCIP and promoter of all of the aforementioned policy and strategies — with a view to investigating the possibility of setting up a training stream as a new activity of the ERNCIP, to take place alongside the core activities (thematic groups and inventory of experimental facilities).

This can be considered as a key moment in the ERNCIP's lifecycle, as the project was initially established under the umbrella of the EPCIP for 2006-2012 (therefore with a

([7]) In the section on preparedness, the following activities, including training, are foreseen: '*We will then support the development of preparedness strategies based around contingency planning, stress tests, awareness raising, training, joint courses, exercises and staff exchange*.'

([8]) See Council conclusions on strengthening chemical, biological, radiological and nuclear (CBRN) security in the European Union — an EU CBRN action plan. The CBRN action plan consists of 124 actions. Its main objective is to complement national measures that address existing gaps and promote exchanges of information and best practices. Available at this link.

([9]) Under Action H.55, the following activities, including training, are foreseen: '… The Member States should develop and conduct, on the basis of risk assessment, regular training at local, regional, and national level.'

strong focus on protection of critical infrastructures) and this new action would call for the embracement of the concept of resilience.

6 Time for action: the initial design of the course

In the second semester of 2014, the activities toward the potential establishment of a pilot training course intensified through the joint work of the ERNCIP and the Academic Committee.

The following high-level requirements were considered necessary in order to take action.

- Identify the competencies required to sustain a safe CIP sector in the EU.
- Establish the current and future needs for these competencies in the EU.
- Develop training and educational programmes designed to develop this range of competencies.
- Develop a range of novel education and training packages that form part of the programme.
- Develop CIP qualifications which will be recognised and accepted across Europe.

'The following items formed part of a possible roadmap.

- Carry out an occupational mapping of the CIP sector to identify the stakeholders (i.e. police, first responders, airports, etc.) and then carry out a survey for each stakeholder in order to estimate the number of employees who would require the training, and the level of training.
- Carry out a functional analysis in order to identify the roles these employees undertake to do their job.
- Write a competency framework for each role.
- Develop a qualification framework with an awarding body.
- Let the training providers write courses which satisfy the competencies.

6.1 Academic Committee meeting of 20 October 2014

The need to discuss those items in greater detail, strongly influenced the agenda as well as the choice of participants to be involved in the Academic Committee's meeting held at the JRC (Ispra) on 20 October 2014.

The meeting incorporated three presentations given by external experts and one video conference, on the following topics:

- '10 reasons to work on a better cyber education' (P. Théron — Thales Group France);
- 'Education and training: an operator's perspective' (G. McQuaid — Vodafone United Kingdom);
- 'Academic program of NIST' (Jennifer Marshall — Katya Delak — William Guy Billotte — National Institute for Standards and Technology — United States);
- Videoconference with Christie Jones and Mark Troutman on 'GMU's critical infrastructure higher education initiative' (Department of Critical Infrastructure Protection and Homeland Security, George Mason University ([10]), VA — United States)

([10]) The CIP/HS has developed comprehensive graduate-level curriculum and supplemental case studies in critical infrastructure security and resilience (CISR). Courses cover topics such as resilience, risk management, information sharing, systems analysis, policies and strategies, cross-sector dependencies and interdependencies, international CISR and cybersecurity. Further information

The presentations triggered brainstorming on the following key aspects:

- the resources and time needed to develop CIPR courses and relative syllabi;
- the type of stakeholders involved in the process of the development;
- the skills the courses are targeting;
- the participation of the students/professionals in such courses;
- the degree of absorption of the graduates by the industry and administration;
- the feedback you receive from alumni or industry on how well graduates fit the available jobs.

What followed was a session on 'European courses and training'. The members of the Academic Committee discussed what could be done towards the development of a harmonised EU training course in the field of critical infrastructure protection and resilience.

Topics and points of view shared can be summarised as follows.

- The organisation of courses in Europe requires more harmonisation of efforts because of the different languages and different approaches of the Member States. At the same time, such conditions should not frustrate universities' freedom to design and develop their courses.
- '*Where should the operators get the talents they need?'* This is a long-term investment that requires a strong multidisciplinary approach with a focus on social science and policy.
- A potential approach for the development of training courses for CIPR professionals could start from mapping the utilities' operational needs together with the public administration and security agencies' ones.
- It is important to have a clear idea of who to reach, what to teach and what message to put forward for professionals in the field of CIPR.
- [It was] proposed that work start with the development of a small training module to be prepared in a short time and with the collaboration of infrastructure operators.
- The importance was highlighted of identifying the professional skills that the course should develop with a view to using such a base to tailor the course content and structure.
- It was also pointed out that the identification of the sectors to be targeted by the course would help with its development.

The last session of the meeting was characterised by joint work that led to the drafting of a document that constituted the very first attempt to lay down the basic structure and the high-level requirements of a potential training course.

> '*Mid-career officials can benefit greatly from thematic courses that are focused on, for them, relevant issues and challenges. Research-based knowledge needs then to be combined with experience-based best-practices. The ambition is here to train motivated professional course participants for higher performance levels following the end of the programme.'*

---

available at this link: https://cip.gmu.edu/education-programs/critical-infrastructure-higher-education-initiative/critical-infrastructure-professional-certificate-program/

Define the skill set:

- *resilience;*
- *crisis management;*
- *cyber;*
- *risk assessment and management, impact analysis and uncertainty analysis;*
- *holistic systemic view;*
- *modelling and simulation;*
- *policy, law and governance (multi-stakeholders and cross-border issues);*
- *system of systems (interdependencies);*
- *system engineering;*
- *business continuity;*
- *testing verification validation;*
- *standardisation, accreditation certification;*
- *societal issues and values and civil protection;*
- *legal and regulatory issues;*
- *ethics;*
- *service and materials logistic and supply chains;*
- *sub-contracting issues and quality/security management of levels of sub-contractors;*
- *safety/security culture and awareness;*
- *decision-making under conflicting objectives (e.g. safety vs security — production vs economy).*

Means of training:

- *lectures to establish common language and framework of knowledge;*
- *exercises;*
- *case studies;*
- *multimedia;*
- *games;*
- *story telling;*
- *blogs;*
- *scenarios;*
- *combined research and experiences;*
- *analysis of failures.*

This exercise enabled the participants to narrow down the principles and elements to be considered in the development of a 'pilot training curriculum for mid-career officials'.

That was also an opportunity for a preliminary and pivotal choice regarding the potential target of the training: mid-career professionals.

This choice was made in order to target professionals that are mid-way between junior and senior positions, in the areas of protection and resilience of critical infrastructure. The main reason for this choice was the assumption that such a target would maximise the impact of the training, as beginners may not be sufficiently acquainted with CIP yet, while seniors may often be engaged in high-level strategic activities.

The assumption, confirmed by the experts and by later consultations with operators and experts, was that mid-career professionals (between 5 and 8 years of work experience) have developed a wider understanding of the field and should still be engaged in duties, like risk analysis or business continuity planning are the ones that can benefit most from a 'view widening' that includes the 'European perspective' (e.g. European grids, transboundary externalities and benefits deriving from joint exercises).

The meeting ended with the creation of a sub-group whose members agreed to summarise the AC's discussion in a short document to be entitled: 'The ERNCIP Academic Committee's proposal on "training for professionals in critical infrastructure protection and resilience"'.

The aim was to use such a report as reference material for a later workshop to be organised through the active involvement of infrastructure operators, with a view to discussing, validating and fine-tuning the proposal, through the inclusion of their functional requirements and expectations.

This would result in a proposal, formulated by academics and subject-matter experts, whose modules would have been further assessed and validated by utilities operating in the European domain.

6.2 The ERNCIP Academic Committee's proposal on 'science-based training for professionals in critical infrastructure protection and resilience'

The proposal drafted by the ERNCIP Academic Committee's sub-group members (Enrico Zio and Paul Theron) was finalised on 28 October 2014. Due to its importance for the promotion and execution of the project, the proposal is attached below in its entirety.

<u>*Executive summary*</u>

This document lays down the contents and structure for the development of training for professionals involved in the safe and secure design, implementation, operation, management and regulation of critical infrastructures, for their protection and resilience against technical failures, man-made attacks and natural damages.

The training courses are intended to involve participants from different critical infrastructures. In this view, important objectives are 'experience-sharing' and 'building of trust' among cross-sectorial and interdependent technologies. In addition, the training and education initiatives can contribute to support the learning and awareness-building about the responsibilities of actors at the different organisations involved in the operation, management and regulation of critical infrastructures. The aim of this proposal is the one of developing a training package — composed of syllabi, course material and use-cases — that will be validated by a network of operators that deliver critical services in the EU context. The work around this proposal will take into account the principles highlighted in the EPCIP framework. More specifically, there will be a particular focus on the requirements expressed in Directive 114/08/EC in terms of the necessary skills required by the Security Liaison Officer's profile.

The operators will be engaged in the preparation of the training's content and structure in view to embed, in the final package, their functional requirements as resulting from nowadays' interconnected and complex infrastructures' lifecycles.

The package, due to the clear aim of embracing a truly multidisciplinary approach, will also include principles of governance, ethics, sociology, economy and law. Such approach will also 'train the trainer' as it will constitute a source of up-to-date and validated material for the upgrade of pre-existing courses.

TRAINING

Target audience of the training programme

Different target audiences require different pedagogical contents and approaches, and different combinations of science-based and experience-based training.

Broadly speaking, we may think of three levels of audiences:

- *Entry-level operators: these professionals are most likely recent graduates from academic programmes, with no or little practical experience, and need to acquire the knowledge and instruction on the basic procedures and practices to smoothly enter into their new field of work. The training programmes tailored for this should, then, be strongly experience-based and the pedagogical approach should be more direct and practical than the conventional academic lecture one: interactive and participatory pedagogics, including simulations, case studies, team projects, should form the backbone of the training.*
- *Mid-career managers or operators: these professionals have already background knowledge and practice upon which they base their work and the training should provide them with new knowledge and understanding helpful for improving their performance. The training programmes tailored for this category of managers/operators should, then, inject research-based knowledge combined with experience-based best practices to provide the opportunity for scientific support to be transformed into improved work practice. The pedagogical approach should allow focusing on work issues and practical challenges that are relevant for the work, combining lecture explanation of the scientific and research-based knowledge and case study and project work for the illustration of the implementation in practical work.*
- *Government decision-makers and business managers: these professionals are concerned with top decisions to be taken under the pressure of responsibility and limited time, often even in acute emergency situations with potential serious consequences for life, environment, business, assets and reputation. On the other hand, their experience, preparation and competence make them fast-learners on matters of their direct interest. In this view, the training programmes tailored to these professionals should refresh them on solutions for better meeting their decision challenges and stimulate them on considering widening their portfolio of views on the decision problems so as to be more confident and robust. The pedagogical approach should allow them to rapidly focus on what is important of the new view of the problem posed and what is interesting of the new solution proposed: for this, it would seem best to proceed with workshops, inter-active seminars and closed session simulations.*

In the following of this proposal, an exercise is made of developing the bases for the training programme of mid-career managers or operators.

Objective of the training programme

The objective is to train mid-career managers or operators on methods, techniques and practices for developing and implementing solutions and strategies for critical infrastructure protection and resilience, within a system-of-systems framework of analysis and a holistic strategic context encompassing risk analysis and prioritisation, risk mitigation and management, performance management,

incident and crisis management, public-private partnerships, organisational, regulatory, legal and ethical issues, information sharing and communication.

The training aims at involving participants from different critical infrastructures, for the benefit of sharing experiences and building trust among players from cross-sectorial and interdependent technologies. In addition, the training can contribute to support the learning and growing the awareness about the responsibilities and roles at the different organisations involved in the operation, management and regulation of critical infrastructures.

Contents of the training programme

The core topics of the training programme should be:

Topic 1: History, concepts, definitions and foundations of critical infrastructure protection and resilience (CIPR)

- Critical infrastructure protection vs civil protection.
- Critical infrastructure protection vs resilience.

Topic 2: CIP policy, legislative and governance frameworks and models

Topic 3: Resilience of critical infrastructures. National, societal, business and technical requirements:

- state of the art and frameworks;
- how critical infrastructures act and react under adverse circumstances: the dynamics of resilience; illustrations from real-life case studies;
- engineering resilience into critical infrastructures: prevision, prevention, protection, recognition, response and recovery capabilities.

Topic 4: Risk assessment and management for CIPR: a panorama of ad hoc disciplines, definitions, standards, methods and use cases, including all-hazards risk analyses (natural, industrial, technical, human, systemic) in large sociotechnical systems

- quality and risk management in third-party sub-contracting relationships: maturity assessment, governance, standards and methods, practical difficulties on the ground.

Topic 5: Complexity and modelling, simulation and analysis of systems and systems-of-systems

Topic 6: Cybersecurity: new threats, new forms of risk management, new legal issues

- Fitting cybersecurity into systems engineering: simple add-on or embedded process?

Topic 7: Logistics and supply chains: between economic performance, complexity, continuity and criminality issues

Topic 8: Inspection, verification, validation and qualification (IVVQ) in systems development

Topic 9: Standardisation, accreditation, certification and homologation: from international and legal aspects including the issue of cyber-trustworthiness (from mere devices to systems)

Topic 10: Crisis management and decision-making in uncertain, fast-paced, complex circumstances.

- models, methods, standards and best practices;

- ethics, legal issues, legal risk management and margins of manoeuvre during crisis: how far can decision-makers go?

Topic 11: Emergency preparedness, culture and awareness raising, exercises and organisational learning

Topic 12: Information sharing and coordination with national authorities and other operators:

- public–private partnership trust circles and information sharing in a context of deregulation, privatisation and national sovereignty issues.

Structure of the training programme

The training programme could include three levels:

- *L1 — 3-day basic training:*

  30-45' lectures on the core topics;

  Interactive classroom discussions on reading material and selected issues;

  Possibly a final exam delivering a basic 'certificate' or 'qualification'.

- *L2 — 5-day intermediate training:*

  Idem plus in-class exercises;

  Possibly a final exam delivering an intermediate 'certificate' or 'qualification'.

- *L3 — Advanced training (5-day training plus coaching support plus final case study presentation):*

  Structured collaborative projects on case studies agreed with the teaching board;

  Report writing and submission;

  Report presentation and delivery an advanced 'certificate' or 'qualification'.

Output of the training programme

It is expected that the mid-career managers and operators attending the course gain new knowledge and improve understanding they can benefit from in the performance of their critical infrastructure protection and resilience activities.

In particular, the programme according to the aforementioned levels should enable the attendants to:

- *integrate or lead a project or management team in charge of CIP and resilience management;*
- *integrate or lead a CIP or resilience engineering team;*
- *Recognise and capture the all-hazards context and system-of-systems dimension of critical infrastructure protection and resilience and see how this applies in the environment they are dealing with;*
- *recognise and understand the multidisciplinary context and dimension of such problems, from technical to organisational, from social to political, from legal to organisational, and characterise how this impacts on and is handled in their specific critical infrastructure protection and resilience area;*

- *identify and compare different strategic and governance approaches for critical infrastructure risk and resilience management;*
- *identify the role of different frameworks of partnerships, systems of information sharing, communication, coordination and collaboration processes;*
- *design, implement and improve CIP and resilience governance, as well as crisis management and emergency preparedness frameworks;*
- *evaluate and use methods of decision-making in the presence of uncertain, adverse circumstances;*
- *identify and compare different methods of modelling, simulation and analysis of risks in interdependent critical infrastructures;*
- *evaluate and manage alternatives for engineering critical infrastructure protection, resilience and cyber resilience;*
- *evaluate and manage processes of certification and homologation, especially with regards to cybersecurity of components and subsystems in complex systems.*

6.3 Focus group meeting on 'mid-career training curriculum in critical infrastructure protection and resilience'

With the Academic Committee's proposal now available, the ERNCIP Office, in collaboration with DG Migration and Home Affairs, organised a focus group meeting, held in Brussels, on 26 February 2015, to involve infrastructure operators in the following discussions:

- overview of existing approaches to training: the added value of the ERNCIP and CIPRNet ([11]);
- presentation of the proposal for mid-career training;
- discussion on Operators' functional requirements for training of mid-career professionals in CIPR, based on the Academic Committee's discussion paper;
- discussion on validation of the training package and use cases;
- requirements for the organisation of a pilot course and organisational issues.

The meeting kicked off with a preliminary introduction to the EPCIP, the operator security plans, the figure of the security liaison officer and the need to focus potential training on 'transboundary' externalities. A preliminary introduction to these items, to be kept as terms of reference, set the ground for a fruitful discussion and joint action toward the design and later execution of a pilot training course based firmly on the EPCIP programme and its principles.

The introductory presentations were followed by an open discussion during which the following topics/items were highlighted.

([11]) The Critical Infrastructure Preparedness and Resilience Research Network, or CIPRNet, establishes a Network of Excellence in Critical Infrastructure Protection (CIP). CIPRNet performs research and development that addresses a wide range of stakeholders including (multi)national emergency management, critical infrastructure operators, policymakers and society. By integrating resources of the CIPRNet partners acquired in more than 60 EU co-funded research projects, CIPRNet will create new advanced capabilities for its stakeholders. A key technology for the new capabilities will be modelling, simulation and analysis for CIP. CIPRNet is building a long-lasting virtual centre of shared and integrated knowledge and expertise in CIP. This virtual centre will provide durable support from research to end users. It will form the foundation for the European Infrastructures Simulation and Analysis Centre (EISAC) by 2020. More information regarding CIPRNet is available at this link: https://www.ciprnet.eu/home.html

- *'Transport security managers do not have the full picture on how to deal with energy and cyber issues and therefore they need training.'*
- *'Operational, management and security employees need training in order to know how to properly react.'*
- *'Security managers have to interact more. So the training has to be about technical but also behavioural topics so they learn to interact with the "outside world".'*
- *'It's difficult to build a security culture within the company. Safety culture has just reached a good level of maturity. Also how to process and assess difficult situations quickly has to be taught. Operators have invoked meetings with stakeholders with a view to learning how to deal with very specific issues.'*

After the initial 'hand-shake', the participants were introduced to the project proposal, through some topics and key questions to be addressed.

- Operators and academia should exchange information on competences and expertise to improve knowledge and awareness of CIP.
- The SLO doesn't have to wait for the threat to come before taking action to implement resilience.
- Training action must respond to operators' need to enhance awareness, experience sharing and trust.
- 'Where to experiment? Who should we direct the training to? We have to reach security managers that need to improve their awareness and methodologies in facing issues related to interdependencies and information sharing.'

The presentation of the training proposal was followed by some information regarding logistics and planning of a potential 'pilot course', to provide an overall picture of the timeframe for the development of the training package that could be followed by the organisation of a pilot course, to be held in the second semester of 2016.

What followed was a long discussion and joint work that enabled the focus group to express their views on how to streamline the seven modules to be included in the training package that was to be developed. The modules were the result of narrowing down the 12 core topics highlighted in the AC's proposal from October 2014. Those core topics have been reworked in view to meeting the operators' functional requirements with a 'client and policy-oriented' approach.

Reaching an agreement regarding the modules and the potential content of the course was not the only challenge discussed by the participants, as other important aspects were considered and analysed.

- Who are the potential participants in such a course? Should the course be dedicated to managers that designate governance models of critical infrastructures? Has the perspective to be the one of the security manager that has to implement the design of security and protection of the infrastructure?
- The course should be slightly multi-faceted and strongly based on protection and resilience.
- The training programme is intended to provide information to a specific target (security managers). Lecturers need to be charismatic and get to the point quickly. Topics should be covered by relevant experts who have direct skills and experience in the field. The training has to look impartial so that participants can adapt and metabolise that interpretation.
- The module on cyber should be focused on Industrial Automation Control Systems (IACS) and not on the IT platform.

- Degrees of criticality vs 'vital infrastructures' should be considered.
- Without pre-course reading and without setting of common vocabulary, the attendants would be 'guessing'. A means of providing this information is strongly suggested. Multimedia should also be considered.
- Setting a common language is important.
- 'Operators suffer insider threats and such factors should also be considered in the course.'
- 'The pre-course material has to clarify what kind of gap you intend to cover.'
- 'We have to collect what exists and structure it in a specific way that meets the criteria of the course.'
- 'Reference to standards is important as they provide guidance and thresholds.'
- 'The training should be built on the most often recurring standards in the field as they are the reference for protection and resilience.'
- 'People that are used to performing risk assessment on a single plant or asset are now often have to assess external dependencies and cascading effects and failures.'
- 'Communication between SLOs working in different organisations has to be facilitated. The module on modelling and complex system has to prepare security managers for the challenges posed in the future.'
- The importance of the interdependencies for the 'image factor' of the company should be considered.
- Corporate social responsibility is important too.
- A toolbox is important regarding the operator security plan if presented in terms of a scheme that refers to standards (scheme of schemes).
- A continuous review of compliance should be included. The OSP must be continuously updated with reference to the evolution of the real world.

At this point in the discussion, the group streamlined the following seven modules.

<u>MODULE 1 — Introduction of the course on CIPR</u>

- CIPEDIA to be used as a glossary and as pre-course material.
- This module to include: explanation of definition of directive, regulation, and recommendation.
- Core topics to be included from the AC's working paper:
    - Topic 1 — History, concepts, definitions and foundations of critical infrastructure protection and resilience (CIPR)
        - Critical infrastructure protection vs civil protection.
        - Critical infrastructure protection vs resilience.
    - Topic 2 — CIP policy, legislative and governance frameworks and models
    - Topic 3 — Resilience of critical infrastructures: national, societal, business and technical requirements: state of the art and frameworks
        - How critical infrastructures act and react under adverse circumstances: the dynamics of resilience; illustrations from real-life case studies.

- Engineering resilience into critical infrastructures: prevision, prevention, protection, recognition, response and recovery capabilities.

MODULE 2 — Complex systems analysis, modelling and simulation

- Core topics to be included from the AC's working paper:
  - Topic 5 — Complexity and modelling, simulation and analysis of systems and systems-of-systems

MODULE 3 — Risk assessment and management

- Core topics to be included from the AC's working paper:
  - Topic 4 — Risk assessment and management for CIPR: a panorama of ad hoc disciplines, definitions, standards, methods and use cases, including all-hazards risk analyses (natural, industrial, technical, human, systemic) in large sociotechnical systems.

MODULE 4 — Risk assessment and management (scenario based)

- This module to be a blend of modules 2 and 3 but strongly based on the following scenarios and potential vectors: cyber, human and natural.

MODULE 5 — Incident response

- Core topics to be included from the AC's working paper:
  - Topic 10 — Crisis management and decision-making in uncertain, fast-paced and complex circumstances;
  - Topic 11 — Emergency preparedness, culture and awareness raising, exercising and organisational learning.

MODULE 6 — The operator security plan

- This module is meant to provide:
  - a toolbox with references to standards and best practices applicable together with hints for continuous review and means of update;
  - a chronological analysis on the evolution of OSP throughout European policies and legislation.
- Core topics to be included from the AC's working paper:
  - Topic 6 — Cybersecurity: new threats, new forms of risk management, new legal issues
    - Fitting cybersecurity into systems engineering: simple add-on or embedded process?
  - Topic 7 — Logistics and supply chains: between economic performance, complexity, continuity and criminality issues
  - Topic 8 — Inspection, verification, validation and qualification (IVVQ) in systems development

- Topic 9 — Standardisation, accreditation, certification and homologation: from international and legal aspects including the issue of cyber-trustworthiness (from mere devices to systems)
- Topic 12 — Information sharing and coordination with national authorities and other operators
    - Public–private partnership trust circles and information sharing in a context of deregulation, privatisation and national sovereignty issues.

MODULE 7 — CI operators' interface with third parties

- This module to include roles and definition of responsibilities and emblematic cases of information exchange.

6.4 Last round of consultations: the ERNCIP Group of EU CIP Experts

The last step, before entering the 'production phase', was the presentation of the project (in the shape it had following the consultation with academics, experts and infrastructure operators) to the ERNCIP Group of EU CIP Experts ([12]), held in Brussels on 9 November 2015.

During this event, the ERNCIP Office gave an update seeking the group's feedback on the proposal, before a wider cascade of information.

Some group members expressed an interest in being involved in the evaluation of the pilot and were later contacted to be involved in the Panel of Observers.

The experts agreed with the ERNCIP's view that the course should be considered as a layer to be added to (and not to conflict with) EU Member States' national means of training related to critical infrastructure protection and resilience.

([12]) The members of this advisory group are nominated by the Member State government authorities responsible for national critical infrastructure protection. The group provides a link to CIP communities in the Member States.

7 Conclusions

The execution of the course was very useful and was much appreciated. The course was also the first of its kind to be entirely dedicated to the European dimension of CIP. Baseline lectures on important topics, approaches to the CIPR issues and experience-based, practical exchanges on these sensitive and complex topics have proven to be important and relevant.

As the section on lessons learned suggests, there is always room for improvements in both the schedule and contents of a course, and also for the inclusion of Europe-specific case studies and exercises.

In a nutshell, improvements in a potential new iteration of the course, apart from the ones described in Section 1.6, should take place in the following areas.

- Further develop the course, to continuously align it with the EPCIP programme and to enable the reporting of experiences that led to transboundary issues being successfully dealt with in all the sectors covered by the policy.
- Make the training a way to consolidate the joint European work around CIP and resilience and to make it widely available.
- Add a full technology-related layer with a view to sharing experiences concerning the fruitful use of specific technology for security and resilience of critical infrastructures.
- Include a more detailed package of pre-course reading material, to be shared in advance, so as to reduce the number of lectures and allow the execution of more table-top exercises, round tables and discussion on very detailed scenarios.
- To facilitate the training of security managers in technical, legal and community engagement issues, involve the following categories of participants:
    - technical staff (e.g. engineers, risk analyst and business-continuity officers);
    - legal staff (e.g. lawyers and social corporate responsibility experts);
    - social media staff.

Future opportunities concerning the 'European dimension of CIP' may allow its extension to be offered to:

- early-career security managers: professionals that have recently graduated from academic programmes and have little or no practical experience;
- government decision-makers: professionals concerned with top decisions to be taken under the pressure of responsibility and limited time, often even in acute emergency situations with potentially serious consequences for life, the environment, business, assets and reputation;
- neighbouring countries and operators of the European Union: to foster the improvement of the 'external domain' of the European programme for critical infrastructure protection (EPCIP). The fact that the EPCIP also aims at reaching out to neighbouring countries of the Union, with a view to establishing CIP-related forms of cooperation, puts the 'training' among the most useful and direct tools to be exploited to achieve such an objective.

The underlying motivation behind the above points is to keep working on the consolidation of knowledge and information advantage right through the 'pyramid' of European CIP, from education to corporate training and to policymaking, to strengthen the robustness and resilience of European infrastructures through a proper safety and security culture, cultivated at all levels, also beyond the European borders.

References

- Communication from the Commission of 12 December 2006 on a European programme for critical infrastructure protection (COM(2006) 786 final — *Official Journal of the European Union* C 126 of 7.6.2007).
- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (*Official Journal of the European Union* L 345/75 of 23.12.2008).
- Commission Staff Working Document on the review of the European programme for critical infrastructure protection (SWD(2012) 190 final — 22.6.2012).
- Commission Staff Working Document on a new approach to the European programme for critical infrastructure protection — Making European critical infrastructures more secure' (SWD(2013) 318 final — 28.8.2013).

List of abbreviations and definitions

AC	Academic Committee
CERT	Computer Emergency Response Team
CIP	critical infrastructure protection
EPCIP	European programme for critical infrastructure protection
ICT	information and communication technology
IT	information technology
JRC	Joint Research Centre (European Commission)
NIST	National Institute of Standards and Technology
OSP	operator security plan
OT	operational technology
SLO	security liaison officer

List of figures

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: http://europea.eu/contact

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

- at the following standard number: +32 22999696, or

- by electronic mail via: http://europa.eu/contact

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: http://europa.eu

EU publications
You can download or order free and priced EU publications from EU Bookshop at: http://bookshop.europa.eu. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see http://europa.eu/contact).

KJ-NA-28657-EN-N

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi 10.2760/932771
ISBN 978-92-79-69731-9